

Since banks and insurance companies, acting as the main structural units of the country's financial system, are at the same time the main channels for the outflow of money into the shadow turnover, it is worth exploring the possibility of developing national standards for cash flow transparency of banks and insurers.

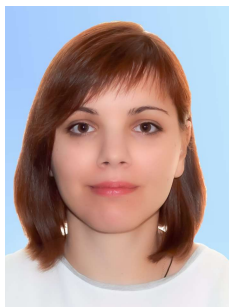
Currently, most banking institutions are in an unstable financial position, so the reliability of such banks is questionable. Shadow operations of banking institutions and insurance companies deprive the national economy of resources for development, and as a result, negatively affect the financial system of the state.

The State Financial Monitoring Service of Ukraine is a central executive body that implements the state policy in the field of prevention and counteraction to legalization (laundering) of proceeds from crime or terrorist financing. It is the effectiveness of the State Financial Monitoring Service of Ukraine that lies in reducing the shadow activities of economic entities in the country.

**Keywords:** financial control, corruption, anti-corruption, prevention, security, shadow economy.

УДК 338.1

DOI 10.31733/2078-3566-2021-2-312-316



**Ольга СТАНІНА**<sup>©</sup>

кандидат технічних наук

(Дніпропетровський державний університет внутрішніх справ)

### ВПЛИВ ДЕЗІНФОРМАЦІЇ НА ЕКОНОМІЧНУ БЕЗПЕКУ КРАЇНИ В УМОВАХ ЦИФРОВИХ ТЕХНОЛОГІЙ

Визначено основну роль інформації в цифровій економіці. Наведено статистичні дані щодо зростання ролі інформації в житті сучасної людини. Визначено поняття дезінформації, її основні види та засоби. Наведено можливі економічні наслідки для окремого підприємства і країни загалом, викликані впливом дезінформації. Окреслено основні функції держави, що стосуються усунення дезінформації. Особливу увагу надано питанню особистої відповідальності за поширення дезінформації та особистої інформаційної та економічної безпеки у світі пост-правди. Запропоновано алгоритм базової перевірки інформації. Зроблено висновки щодо ролі медіаграмотності у питанні безпеки кожної конкретної країни, підприємства і особистості.

**Ключові слова:** інформаційна безпека, економічна безпека, інформація, дезінформація, цифрова економіка, фейкові новини.

**Постановка проблеми.** На сьогодні використання цифрових технологій стає важливим показником економічного розвитку країни. Цифрова економіка має сильний вплив не тільки на державу та підприємства, але й на життя звичайних громадян. Як показують деякі наукові дослідження [1], у майбутньому у світі поступово буде збільшуватися доля інформаційних систем та технологій в різноманітних галузях людської діяльності. Штучний інтелект, робототехніка, доповнена реальність, хмарні технології тощо надалі будуть мати все більший вплив на економіку країни зокрема та світу загалом.

Після 1990-х, разом із поширенням мережі «Інтернет» світом, кількість інформації, з якою ми стикаємося щоденно, зростає у геометричній прогресії. Сьогодні ж людська залежність від інформації стає все більшою. Згідно зі сумісним звітом We Are Social та Hootsuite «Digital 2020» [2], станом на 2020 рік на планеті зафіксовано приблизно 7,67 млрд людей, і серед них майже 5,19 млрд (тобто 67 %) користуються мобільним телефоном (смартфоном), 4,54 млрд (59 %) виходять за пошуком інформації до мережі «Інтернет», а 3,8 млрд (тобто майже половина – 50 %) – активні користувачі соціальних мереж. До того ж, згідно з даними виконаних досліджень, середньостатистична людина майже 40 % свого часу віддає перевагу відпочинку саме в Інтернеті.

З усіма цими змінами, що відбуваються тепер у світі, саме інформація стала найбільшою цінністю, адже вона дає змогу контролювати різноманітні процеси. Інформація всюди,

© Станіна О.Д., 2021

ORCID iD: <https://orcid.org/0000-0001-6754-0317>

[st.olga.d@gmail.com](mailto:st.olga.d@gmail.com)

і сьогодні за її безпосередньої допомоги можна заводити нові контакти, створювати цілі системи чи навіть встановлювати свої власні правила гри.

Проте, як відомо, будь-яка перевага обертається для свого користувача можливими недоліками та загрозами. І, на жаль, процес поширення та зростання ролі інформації у світі це негласне правило не обійшло. Розвиток Інтернету як цифрової копії відомого нам світу і соціальних мереж як його невід'ємних частин, що захопили увагу половини людства, насправді, призвів до геометричного зростання дезінформації та фейкових новин.

**Аналіз публікацій, в яких започатковано вирішення цієї проблеми.** На Заході питання взаємного впливу економіки та інформаційних технологій вивчало немало дослідників, серед яких, наприклад, Л. Соеті, Е. Жуст, Дж. Бругель, А. Сіерер, М. Поджола, В. Дейл, С. Джоншер. Одночасно над вивченням проблем цифрової економіки працювали вчені, як-от Х. Альбах, О. А. Джусов, П. Догерті, Н. М. Краус, С. Маркович, Т. Нібел, Т. Д. Сіташ, К. Шваб. Серед науковців, що займаються останнім часом питаннями дезінформації, треба назвати: Д. Донована, Х. Дж. Ларсона, Ф. Менцера, Д. Г. Ренда, М. Хамелеерса, Е. Хумпрехт та ін.

**Метою** статті є вивчення впливу дезінформації на економічну безпеку країни та надання рекомендацій щодо запобігання її негативних наслідків.

**Виклад основного матеріалу.** Більшість з нас так чи інакше стикалася з дезінформацією під час перегляду телебачення, різних відеороликів на відомих відеохостингах, читання новин, спілкування в соціальних мережах тощо. Але дезінформація здебільшого призначена не стільки для того, щоб впливати на кожну конкретну особистість окремо, скільки на соціальні та економічні відносини загалом.

Спочатку визначимо саме поняття «дезінформації». Згідно зі словником української мови, під «дезінформацією» розуміють певні дії особистості, які призвели до введення в оману іншу людину внаслідок передачі неправдивої інформації. В деяких джерелах під дезінформацією розуміють спотворену, свідомо неправдиву інформацію, але при такому позначенні губиться важливий пласт інформації щодо можливості несвідомої передачі неправдивих свідчень. Тому надалі будемо використовувати більш широке розуміння цього поняття.

В іноземній літературі [3] зазвичай виокремлюють два типи дезінформації:

1) випадкова дезінформація (misinformation), до якої треба відносити всю неправдиву інформацію, що була поширена особою, яка про це не знала (тобто ненавмисна);

2) дезінформація (disinformation) – сюди вже належить уся неправдива інформація, що була поширена особою, яка знала про це заздалегідь (тобто умисна).

Іноколи також окремим типом виділяють ще й шкідливу інформацію (mal-information), тобто правдиву інформацію, яка використовується спеціально для заподіяння шкоди людині, організації або країні (прикладом такого виду інформації може бути поширення в соціальних мережах особистої розмови відомої особи для підриву її репутації).

Відома у світі організація UNESCO у своєму довіднику з журналістської освіти [4] виділяє такі засоби дезінформації:

1. Сагира та пародія. На перший погляд, такий вид інформаційних ресурсів, здається, доданий до списку помилково, але при більш детальному розгляді приходять усвідомлення, що за неправильного розуміння контексту така інформація стає повним аналогом випадкової дезінформації.

2. «Сенсаційні» заголовки або так звані клікбейти. Зрозуміло, що в час жорсткої конкуренції за аудиторію редактори змушені вигадувати нові способи привертання уваги, але тоді, коли людина продивляється лише заголовки новин, не вчитуючись у сам їх зміст (що на практиці достатньо часто й відбувається), маємо дезінформацію.

3. Зміст, що вводять в оману. На жаль, досить часто вживаний вид дезінформації, яким користуються, наприклад, недобросовісні журналісти. Особливістю цього варіанта неправдивої інформації є навмисне спотворення початкової інформації. Прикладом таких «новин» може бути фотокартка, яка була певним чином обрізана, неповна цитата тощо. Сюди ж можна віднести рекламний контент без відповідної позначки.

4. Неправдивий контент. До цього виду дезінформації належить правдива інформація, яка використовується в іншому контексті. Наприклад, фотокартка, яка була зроблена під час війни в одній країні, розповсюджується через багато років згодом в іншій як «свіжа» новина.

5. Контент самозванця або плагіат новини, фото, інформації тощо.

6. Маніпульований зміст. Неправдива новина для зміни думки читача щодо тієї чи іншої інформації або особистості.

7. Сфабрикований контент. Повністю фейкова (тобто неправдива) новина для маніпуляції думками читачів.

Розглянемо на прикладі комерційного підприємства, як дезінформація може вплинути

на економічну безпеку:

– дії (або ж бездіяльність) працівників, спрямовані на підрив репутації підприємства, що може призвести до прямих негативних економічних наслідків (ці дії не обов'язково мають бути умисними) у вигляді нанесення шкоди майну, загрози непередбаченого зниження собівартості активів або навіть втрати економічної незалежності;

– конфлікти, викликані «війною» (можливо, інформаційною) з прямими конкурентами;

– реклама (можливо, навіть агресивна), яка може заподіяти шкоду (у тому числі економічного характеру) самому підприємству і його конкурентам;

– нечесна «гра» і «непрозорі» відносини з працівниками, партнерами і конкурентами, які руйнують процеси налагодження позитивної взаємодії, що прямо пов'язано з подальшою економічною безпекою кожного з перерахованих учасників бізнесу.

– неправильне розуміння ситуації, і, як наслідок, конфлікти з конкурентами або, навпаки, робота на конкурента;

– наявність прихованих форм впливу;

– погіршення загального іміджу або формування негативної громадської думки про окреме підприємство чи країни загалом.

Звичайно, перше питання, яке треба ставити у контексті фейкових новин – це питання про те, кому це цікаво. Але тут потрібно розуміти і таке: крім самого творця фейкової новини (у якого можуть бути найрізноманітніші причини створення такої інформації), у кожній неправдивій новині обов'язково є агенти поширення, і вони не завжди до кінця усвідомлюють свою роль у поширенні дезінформації.

Особливо критичною дезінформація стає тоді, коли вона безпосередньо стосується здоров'я людини. І в цьому сенсі треба зазначити усвідомленість Європейського Союзу. Тож по мірі поширення різноманітних фейкових новин щодо COVID-19, Європейська Комісія та Верховний Представник 10 червня 2020 року випустили сумісне повідомлення щодо боротьби з дезінформацією [5], у якому не просто засудили подібні новини, але й запропонували низку конкретних дій, спрямованих на зниження кількості неправдивих новин та підвищення стійкості громадян ЄС до дезінформації. Серед запропонованих дій було посилення співпраці з вченими, що займаються перевіркою фактів, та з міжнародними партнерами, включно з ВООЗ; також передбачалися перевірки діяльності онлайн-платформ у контексті поширення правдивої інформації, яка стосується коронавірусу тощо.

Але, на жаль, у середньому боротьба з дезінформацією на рівні держав не є такою злагодженою та демократичною, як у випадку із ситуацією щодо COVID-19. Як стверджують автори статті [6], з кожним новим роком збільшується кількість маніпуляцій інформацією у соціальних сферах. Наприклад, у 2020 році, якщо робити порівняння отриманих показників з відомостями за минулий рік, на 15 % зросла кількість держав, в яких використовують дезінформацію для досягнення політичних цілей або інформаційної пропаганди.

Для блокування поширення оманливої інформації різні держави використовують найрізноманітніші методи, починаючи від створення відповідного законодавства для запобігання дезінформації і закінчуючи закриттям тих чи інших інформаційних ресурсів та навіть відключенням доступу до мережі «Інтернет». Зрозуміло, що більшість країн намагається віднайти деякий баланс між крайнощами – жорстким контролем руху інформації та збереженням статус-кво.

Якщо ж говорити про можливі та бажані функції держави у вирішенні проблеми поширення дезінформації, то можна виокремити такі:

– чітко визначена публічна позиція щодо протидії поширенню дезінформації;

– формування правового поля та запровадження ефективних санкцій за порушення його положень;

– організація та фінансування наукових праць, присвячених проблемам впливу, поширенню та протидії дезінформації;

– організація навчання осіб, які обіймають виборні посади, та дипломатів щодо можливостей впливу дезінформації та методів протидії її поширенню;

– координування діяльності структур у сфері медіаграмотності;

– координування міжнародної співпраці українських представників інформаційного бізнесу з європейськими колегами щодо протидії дезінформації.

Однак покладатися лише на можливості держави чи конкретного підприємства у питанні інформаційної безпеки може бути хибним вибором. Тому коли йдеться про перевірку інформації на правдивість, треба не забувати про свою особисту відповідальність, і здатність до критичного мислення в такій справі буде вирішальною.

У статті 302 Цивільного кодексу України [7] закріплено: «Фізична особа, яка поши-

рює інформацію, зобов'язана переконатися у її достовірності. Фізична особа, яка поширює інформацію, отриману з офіційних джерел, не зобов'язана перевіряти її достовірність та не несе відповідальності в разі її спростування. Фізична особа, яка поширює інформацію, отриману з офіційних джерел, зобов'язана робити посилання на таке джерело». Проте як часто на практиці ми перевіряємо отриману інформацію?

Боротьба з фейковою інформацією максимально ускладнюється, коли приходять розуміння, що переважно саме читачі відіграють головну роль у питанні перенесення брехні. Звичайний споживач інформації не шукає фактів – він зі спокійним обличчям самостійно поширює фейки, оскільки вони більше відповідають його моделі світу [8].

Кожен день, так само просто, як ми шукаємо інформацію в Інтернеті, ми можемо її туди додавати. На практиці маємо справу з поширеною серед користувачів ситуацією, коли та чи інша інформація, яка була розміщена на просторах «Світового павутиння», насправді є лише особистою думкою тієї чи іншої людини і ніяк не стосується правди.

Тому після читання новин треба обов'язково їх перевіряти на правдивість, аналізувати твердження за допомогою іншої відкритої інформації, зіставляти отримані відомості та робити висновки щодо їх правдивості. Алгоритм першочергової перевірки інформації на правдивість стисло можна описати так:

1. Оберіть ту інформацію, яка вас цікавить і в якій ви не впевнені.
2. Оцініть актуальність обраної інформації (є немала вірогідність того, що та інформація, яка була правдивою 10 років тому, зараз вже змінилася).
3. Спробуйте знайти першоджерело цієї інформації та оцінити його достовірність.
4. Зверніться до офіційного джерела.
5. Знайдіть потрібну інформацію в альтернативних джерелах і зіставте її з даними з офіційного джерела і початковою інформацією, яку ви перевіряєте.
6. Спробуйте знайти першочергову інформацію в контексті, можливо, залежно від нього вона буде змінювати свою суть.
7. Зіставте всю отриману інформацію та зробіть висновок щодо правдивості чи хибності новини.

Безумовно, якісна та повна перевірка інформації на достовірність, її верифікація – процес досить складний та довгий, особливо тоді, коли інформація, що перевіряється, є умисною дезінформацією. Але уважність і пильність можуть допомогти вчасно скоригувати свої дії відповідно до реального стану справ.

**Висновки.** Сьогодні інформація є чи не найбільш цінним ресурсом в економіці для ухвалення управлінських рішень. Але в умовах глобальної цифровізації все складніше стає відрізнити достовірність тих чи інших даних. Використання дезінформації для отримання прибутку, навмисної омані чи отримання певної політичної вигоди в будь-якому разі буде мати негативний наслідок для економіки країни, конкретного підприємства чи певної людини. Тому питання медіаграмотності й здатності захиститися від фальшивої інформації або новин сьогодні стає не тільки питанням безпеки країни чи комерційної організації, а й глобальною проблемою та невідкладним завданням кожної конкретної людини.

#### Список використаних джерел

1. IDC – Global ICT Spending. Forecast 2020–2023. URL : <https://www.idc.com/promo/global-ict-spending/forecast>.
2. Simon Kemp. Digital 2020: 3.8 billion people use social media. URL : <https://wearesocial.com/blog/2020/01/digital-2020-3-8-billion-people-use-social-media>.
3. Stahl B. C. On the Difference or Equality of Information, Misinformation, and Disinformation: A Critical Research Perspective. URL : <http://www.inform.nu/Articles/Vol9/v9p083-096Stahl65.pdf>.
4. Ireton C., Posetti J. Journalism, 'Fake News' & Disinformation. Handbook for Journalism Education and Training. URL : [https://en.unesco.org/sites/default/files/journalism\\_fake\\_news\\_disinformation\\_print\\_friendly\\_0.pdf](https://en.unesco.org/sites/default/files/journalism_fake_news_disinformation_print_friendly_0.pdf).
5. Coronavirus: EU strengthens action to tackle disinformation. URL : [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_20\\_1006](https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1006).
6. Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation. URL : <https://demtech.oii.ox.ac.uk/research/posts/industrialized-disinformation/#continue>.
7. Про внесення змін до Цивільного кодексу України щодо права на інформацію : Закон України від 22 груд. 2003 р. № 3261-IV.
8. Почепцов Г. Г. Дезінформація. Київ : вид-во А. В. Паливоди, 2019. 248 с.

Надійшла до редакції 09.06.2021

### References

1. IDC – Global ICT Spending. Forecast 2020–2023. URL : <https://www.idc.com/promo/global-ict-spending/forecast>.
2. Simon Kemp. Digital 2020: 3.8 billion people use social media. URL : <https://wearesocial.com/blog/2020/01/digital-2020-3-8-billion-people-use-social-media>.
3. B. C. Stahl. On the Difference or Equality of Information, Misinformation, and Disinformation: A Critical Research Perspective. URL: <http://www.inform.nu/Articles/Vol9/v9p083-096Stahl65.pdf>.
4. Ireton C., Posetti J. Journalism, 'Fake News' & Disinformation. Handbook for Journalism Education and Training. URL: [https://en.unesco.org/sites/default/files/journalism\\_fake\\_news\\_disinformation\\_print\\_friendly\\_0.pdf](https://en.unesco.org/sites/default/files/journalism_fake_news_disinformation_print_friendly_0.pdf).
5. Coronavirus: EU strengthens action to tackle disinformation. URL : [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_20\\_1006](https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1006).
6. Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation. URL: <https://demtech.oii.ox.ac.uk/research/posts/industrialized-disinformation/#continue>.
7. Pro vnesennia zmin do Tsyvilnoho kodeksu Ukrainy shchodo prava na informatsiiu [On amendments to the Civil Code of Ukraine regarding the right to information] : Zakon Ukrainy vid 22 hrud. 2003 r. № 3261-IV. [in Ukr].
8. Pocheptsov, H. H. (2019) Dezinformatsiia [Misinformation]. Kyiv : vyd-vo A. V. Palyvody. 248 s. [in Ukr].

### ABSTRACT

**Olha Stanina. The impact of information and misinformation on the economic security of the country in the digital economy.** The article outlines the fundamental role of information in the modern digital economy. Statistical data on the growing role of information in the life of modern man is presented. The concept of misinformation, its main types (misinformation, disinformation, and mal-information), and means (such as satire, false connection, misleading content, false context, imposter content, manipulated content, and fabricated content) are defined. Possible economic consequences for an individual enterprise and the country as a whole, caused by the influence of misinformation, are given. The experience of the European Union in the field of misinformation prevention is presented on the instance of the development of events related to covid-19. It is emphasized that in the period between 2019 and 2020, the number of countries in which information is manipulated has increased by 15%. The main functions of the state concerning the elimination of misinformation are outlined. Particular attention is paid to the issue of personal responsibility for spreading misinformation, personal information, and economic security in the post-truth world. Furthermore, the article focuses on the fact that the dissemination of misinformation is not always conscious and that often the spreader of disinformation is a person who has not checked the reliability of transmitted information sources. A basic algorithm for checking the reliability of information is offered, and the role of care and vigilance is emphasized. Conclusions are drawn on the role of media literacy and critical thinking skills in the security of each particular country, enterprise, and individual.

**Keywords:** *information security, economic security, information, misinformation, digital economy, fake news.*